Tina Wolfson, CA Bar No. 174806
twolfson@ahdootwolfson.com
Robert Ahdoot, CA Bar No. 172098
rahdoot@ahdootwolfson.com
Theodore Maya, CA Bar No. 223242
tmaya@ahdootwolfson.com
Bradley K. King, CA Bar No. 274399
bking@ahdootwolfson.com
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: (310) 474-9111
Fax: (310) 474-8585

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BARBARA TREVINO, individually and on behalf of all others similarly situated,

Plaintiff,

v.

EQUIFAX, INC.; and DOES 1-50,

Defendant.

No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Barbara Trevino ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Equifax Inc. ("Equifax" or "Defendant"), and alleges as follows:

NATURE OF THE CASE

1. On September 7, 2015, Equifax announced a "Cybersecurity Incident" (hereinafter, the "Data Breach") affecting, according to its own account, "approximately 143 million U.S. consumers." <https://www.equifaxsecurity2017.com> (last visited Sept. 7, 2017).

2. "The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed." *Id.*

3. Such information is among the most highly sensitive personally identifiable information ("PII") that exists concerning U.S. consumers, and can be used by criminals to open fraudulent financial accounts in such consumers' names, encumber consumer's property, commit tax fraud, and commit a variety of financial crimes with severe consequences for the victims.

4. In its press release concerning the Data Breach, Equifax stated that "the unauthorized access occurred from mid-May through July 2017." *Id.*; *see also* <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628> (last visited Sept. 7, 2017).

5. Equifax also admitted that it discovered the "unauthorized access" on July 29, 2017, though it did not notify those whose PII was compromised in the Data Breach about it until September 7. *Id.*

6. Only two days after Equifax discovered the Data Breach, on August 2, 2017, Equifax's Chief Financial Officer John Gramble sold more than 13 percent of his holdings in Equifax; Joseph Loughran, president of U.S. information solutions, sold 9

percent of his holdings; Rodolfo Ploder, president of workforce solutions, sold 4 percent of his holdings. None of the filings list these transactiosn as being part of 10b5-1 scheduled trading.

7. Through a video statement from Defendant's then-Chairman and Chief Executive Officer, Richard F. Smith, Equifax admitted that the Data Breach "strikes at the heart of who we are and what we do," because "[w]e pride ourselves on being a leader in managing and protecting data." *Id.*

8. At the same time it released these statements concerning the Data Breach, Equifax offered "Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers," ("TrustedID Premier") but Equifax only offered such assistance for one year, despite that the compromised PII can be used to injure victims of the Data Breach long after one year has passed. *Id.* In addition, the product offered is Equifax's own product, which is not as robust as certain competing products, and Equifax most likely will encourage consumers to purchase additional protection once the initial year of coverage expires. Moreover, such products typically only look for fraud involving new accounts, but do little or nothing to prevent fraud on consumers' existing accounts.

9. Equifax has established a dedicated call center, but by its own admission the high volume of calls has created long wait lines, busy signals, and dropped calls. <https://www.equifaxsecurity2017.com/frequently-asked-questions/#tab-2> (last visited Sept. 28 2017).

10. Equifax provided a website, www.equifaxsecurity2017.com, where consumers could input their identifying information and be told whether, to Equifax's knowledge, their PII was compromised in the Data Breach. Consumers are supposed to be able to enroll in the TrustedID Premier product from www.equifaxsecurity2017.com. However, Equifax is "currently experiencing difficulties with our TrustedID website. As a result, the site may be unavailable periodically."

11. On September 27, 2017, Equifax's Interim Chief Executive Officer Paulino do Rego Barros Jr. published an opinion piece in the Wall Street Journal admitting that

"[w]e were hacked. That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key consumer questions were too often delayed, incomplete, or both." <https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253> (last visited Sep. 28, 2017).

12. That the intruders were able to access such a large amount of sensitive consumer data via a vulnerability in the company's Web site suggests that Equifax may have fallen behind in applying security updates to its Internet-facing Web applications.

13. On September 13, 2017 Equifax released a statement that "[t]he attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application." <https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/> (last visited Sept. 27, 2017).

14. The Apache Software Foundation ("ASF") is a US 501(c)(3) charitable organization that develops freely available, open-source software, including Apache Struts (CVE-2017-5638), used by Equifax. <https://apache.org/foundation/> (last visited Sept. 27, 2017).

15. On September 14, 2017, ASF released a statement explaining that a vulnerability was found in Apache Struts (CVE-2017-5638), that this vulnerability "was originally reported on 7 March 2017," and, that "[t]his vulnerability was patched on 7 March 2017, the same day it was announced." In its statement, ASF concluded that "the Equifax data compromise was due to their failure to install the security updates provided in a timely manner." <https://blogs.apache.org/foundation/entry/media-alert-the-apache-software> (last visited Sept. 27, 2017)

16. This is not the first time Equifax suffered a data breach. In May 2017, hackers exploited lax security at Equifax's TALX payroll division, which provides

online payroll, Human Resources, and business tax services, thus gaining access to consumers' highly sensitive federal tax forms, Social Security Numbers, and other sensitive PII. *See* <https://oag.ca.gov/system/files/Allegis%20-%20CA%20Templates_0.pdf> (last visited Sept. 7, 2017); <https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/> (last visited Sept. 7, 2017).

17. The Data Breach only could have occurred because Equifax failed to implement adequate security measures to safeguarded consumers' PII. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a large number of individuals' valuable personal and financial information.

18. Armed with the personal information obtained in the Data Breach, identity thieves can commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, and open financial accounts and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other criminals who intend to misuse the information.

19. As a result of Equifax's failure to prevent the Data Breach, Plaintiff and Class members are exposed to a heightened, imminent risk of fraud, identity theft, and financial harm, as detailed below. Plaintiff and Class members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur, out-of-pocket costs for obtaining credit reports, credit freezes, more robust credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's impact on their PII for the remainder of their lives. Class members will have

to spend considerable time and money for the rest of their lives in order to detect and respond to the impact of the Data Breach.

20. Plaintiff brings this action to remedy these harms individually and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further credit monitoring services with accompanying identity theft insurance beyond Equifax's current one-year offer, and injunctive relief including an order requiring Equifax to implement improved data security measures.

PARTIES

21. Plaintiff Barbara Trevino is a resident of Los Angeles, California. On September 7, 2017, Plaintiff was informed by Equifax that, "[b]ased on the information [she] provided [through Equifax's www.equifaxsecurity2017.com website], we believe that [her] personal information may have been impacted by [the Data Breach]."

22. Defendant Equifax, Inc. is incorporated in Georgia, with its headquarters located at 1550 Peachtree Street, N.W., Atlanta, Georgia.

23. Equifax is one of the major credit reporting bureaus in the United States. As a credit bureau service, "[t]he company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide." Equifax 2016 Annual Report at 2. Equifax prides itself as a leader in "Big Data." *Id.* at 7. As a credit bureau, Equifax maintains information related to the credit history of consumers and provides the information to creditors who are considering a borrower's application for credit or who have extended credit to such consumers.

JURISDICTION AND VENUE

24. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiff brings claims under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681e, *et seq.*

25. This Court also has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendant.

26. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and regularly transacts business in California and within this District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Plaintiff resides in this District, Defendant regularly transacts business here, and many Class members reside in this District.

ADDITIONAL FACTS

A. Equifax Promised to Protect Class Members' PII, but Maintained Inadequate Data Security

28. Prior to the Data Breach, Equifax promised its customers and everyone whose PII it collects that it would reasonably protect their PII. Equifax publishes numerous privacy policies, and proudly declares that: "For more than 100 years, . . . [w]e have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. . . . Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."

29. As a credit bureau Equifax is obligated by federal law to protect consumers' PII, including under the Fair Credit Reporting Act ("FCRA"), and the Gramm-Leach-Bliley Act ("GLBA").

30. Plaintiff and Class members had no choice in Equifax's collection, maintenance, and ultimate disclosure of their PII. Rather, Equifax was allowed to perform such services, involving such sensitive information only if it adhered to the requirements of laws meant to protect the privacy of such information, such as the FCRA and the GLBA. Equifax's maintenance, use, and furnishing of such PII is and

was intended to affect Plaintiff and Class members, and the harm caused by disclosure of that PII in the Data Breach was entirely foreseeable to Equifax.

B. The Data Breach Has Exposed Plaintiff and Other Consumers to Fraud, Identity Theft, Financial Harm, and a Heightened, Imminent Risk of Such Harm in the Future

31. On its website, Equifax "recommend[s] that consumers be vigilant in reviewing their account statements and credit reports." <https://www.equifaxsecurity2017.com/frequently-asked-questions/> (last visited Sept. 7, 2017).

32. There is a strong likelihood that Class members already have or will become victims of identity fraud given the breadth of their PII that is now publicly available.

33. For instance, Javelin Strategy & Research, a consulting firm that specializes in fraud and security, reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal." <https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy> (last visited April 14, 2016).

34. Equifax's creation of the www.equifaxsecurity2017.com website itself has created further threats to consumers and their PII. Because the website is not hosted on Equifax's company domain, equifax.com, it is easy to create fake versions of the site. Like www.equifaxsecurity2017.com, these fake sites also prompt consumers to enter their PII, including last name and Social Security number, furthering the exposure and risk to consumers. This risk is not merely hypothetical. At least one such fake version already was created. To demonstrate how unsecured www.equifaxsecurity2017.com is,

software engineer Nick Sweeting created one such fake website, www.securityequifax2017.com. The site received almost 200,000 visits before it was taken down. The fraud is so convincing that on three separate occasions Equifax itself posted links to the imitation website through Equifax's Twitter account. These posts have since been deleted.

35. The exposure of Plaintiff's and Class members' Social Security numbers in particular poses serious problems. Criminals frequently use Social Security numbers to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Even where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start."[1] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.

36. As a result of the Data Breach, Plaintiff and Class members face the following injuries:

- identity fraud and theft, including unauthorized bank activity, fraudulent credit card purchases, and damage to their credit;
- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of PII;
- loss of the opportunity to control how their PII is used.
- loss of use of and access to their financial accounts and/or credit;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

[1] Social Security Administration, Identity Theft and Your Social Security Number, pp. 7-8, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 7, 2017).

- loss of access to new credit, and/or increased time and money being required to get new credit, following implementation of credit freezes;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- money, including fees charged in some states and time spent placing fraud alerts and security freezes on credit records;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- costs of credit monitoring that is more robust than the services being offered by Equifax;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services once the temporary services being offered by Equifax expire;
- costs and lost time from dealing with the consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate steps to protect adequately the PII in its possession.

37. The risks that Plaintiff and Class members bear as a result of the Data Breach cannot be mitigated by the credit monitoring Equifax has offered to affected consumers because it can only help detect, but will not prevent, the fraudulent use of

Class members' PII. Instead, Plaintiff and Class members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Class members.

38. The risks borne by affected consumers are not hypothetical: Equifax has admitted that Class members' personal information was disclosed in the Data Breach, has admitted the risks of identity theft, and has encouraged consumers to vigilantly monitor their accounts.

C. Equifax Was Required to Implement Reasonable Security, and to Investigate and Provide Timely and Adequate Notification of the Data Breach

39. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to ***insure the security and confidentiality of customer records and information***;
>
> (2) to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and
>
> (3) to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b) (emphasis added).

40. In order to satisfy their obligations under the GLBA, financial institutions must "develop, implement, and maintain a comprehensive information security program

that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4. "In order to develop, implement, and maintain [their] information security program, [financial institutions] shall:

> (a) Designate an employee or employees to coordinate [their] information security program.
>
> (b) ***Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information*** that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [their] operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) ***Design and implement information safeguards to control the risks [they] identify through risk assessment***, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> (d) Oversee service providers, by:
>
> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

> (2) Requiring [their] service providers by contract to implement and maintain such safeguards.
>
> (e) ***Evaluate and adjust [their] information security program in light of the results*** of the testing and monitoring required by paragraph (c) of this section; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program."

Id.

41. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* "At a *minimum*, an institution's response program should contain procedures for the following:

> a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
>
> b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
>
> c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
>
> d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and

e. Notifying customers when warranted.

Id. (emphasis added).

42. Furthermore, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *See id.*

43. Credit bureaus are "financial institutions" for purposes of the GLBA, and are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, *Bank Holding Companies and Change in Bank Control*, "credit bureau services"[2] are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." Because Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

44. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

45. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to (a) implement and

[2] Credit bureau services include "[m]aintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower." *See* 12 C.F.R. § 225.28.

maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Class members' PII.

46. Upon information and belief, Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" as mandated by the GLBA. This includes, but is not limited to, Equifax's failure to notify affected individuals themselves of the Data Breach in a timely and adequate manner.

CLASS ACTION ALLEGATIONS

47. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

48. Plaintiff brings claims as specified below on behalf of a proposed nationwide class ("Nationwide Class"), preliminarily defined as follows:

> All natural persons and entities in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.

49. Plaintiff also brings claims as specified below on behalf of a California statewide subclass (the "California Subclass"), preliminarily defined as follows:

> All natural persons and entities in California whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.

50. Except where otherwise noted, "Class members" shall refer to members of the Nationwide Class and the California Subclass, collectively, and all classes are

referred to collectively as the "Classes."

51. Excluded from the Nationwide Class and the California Subclass are Defendant and its current employees, as well as the Court and its personnel presiding over this action.

52. The Nationwide Class meets the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3).

53. **Numerosity:** The Classes are so numerous that joinder of all members is impracticable. According to Equifax, the Data Breach affected approximately 143 million U.S. consumers.

54. **Commonality:** There are numerous questions of law and fact common to all Class members, including but not limited to the following:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant owed a duty to Plaintiff and Class members to adequately protect their PII;
- whether Defendant breached its duties to protect the PII of Plaintiff and Class members;
- whether Defendant knew or should have known that its data security systems and processes were vulnerable to attack;
- whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of PII;
- whether Defendant violated the FCRA, the GLBA, and/or state data breach laws; and
- whether Plaintiff and Class members are entitled to equitable relief including injunctive relief.

55. **Typicality:** Plaintiff's claims are typical of the claims of Class members. Plaintiff, like all proposed Class members, had his PII compromised in the Data Breach.

56. **Adequacy:** Plaintiff will fairly and adequately protect the interests of all

Class members. Plaintiff has no interests that are adverse to, or in conflict with, other Class members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

57. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Classes predominate over any questions which may affect only individual Class members.

58. **Superiority:** The proposed Classes also meet the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

59. Absent a class action, the majority of Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

60. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the PII of the Class members and other individuals, and varying adjudications could establish incompatible standards with respect to: Defendant's duty to protect individuals' PII; whether Defendant's ongoing conduct violates the FCRA and/or other state or federal law; and whether the injuries suffered by Class members are legally cognizable. Prosecution of separate actions by individual Class members would also create a risk of individual adjudications that would be dispositive of the

interests of other Class members not parties to the individual adjudications, or substantially impair or impede the ability of Class members to protect their interests.

61. **Injunctive Relief:** In addition, Defendant has acted and/or refused to act on grounds that apply generally to all Class members, making injunctive and/or declaratory relief appropriate with respect to all Classes under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the PII of Class members, (2) fails to adequately protect their PII, and (3) violates Class members' rights under the FCRA and other claims alleged herein.

62. **Certification of Particular Issues:** In the alternative, this action may be maintained as class actions with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

CAUSES OF ACTION

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

(on behalf of the Nationwide Class)

63. Plaintiff incorporates by reference all paragraphs above.

64. As individuals, Plaintiff and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

65. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

66. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

67. As a consumer reporting agency, Equifax is required under the FCRA to

"maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

68. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

69. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

70. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

71. Equifax furnished the Nationwide Class members' consumer reports by: disclosing their consumer reports to unauthorized entities and hackers; allowing unauthorized entities and hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or hackers from accessing their

consumer reports.

72. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.[3]

73. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) of the FCRA by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. Equifax was well aware of the importance of the measures organizations like it should take to prevent data breaches, and willingly failed to take them.

74. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See*, *e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of its duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other Class members of their rights under the FCRA.

75. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and Nationwide Class members' personal information for no permissible purposes under the FCRA.

[3] *E.g.*, Statement of Commissioner Brill (Federal Trade Commission 2011), *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf> (last visited Sept. 7, 2017).

76. Plaintiff and Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

77. Plaintiff and Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(on behalf of the Nationwide Class)

78. Plaintiff incorporates by reference all paragraphs above.

79. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

80. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and other Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

81. Plaintiff and Nationwide Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

82. Plaintiff and Nationwide Class members are also entitled to recover their

costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III

NEGLIGENCE

(on behalf of the Nationwide Class)

83. Plaintiff incorporates by reference all paragraphs above.

84. Equifax owed a duty to Plaintiff and Class members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class members' information was adequately secured from unauthorized access.

85. Equifax's privacy policy, and other public statements, acknowledged its duty to adequately protect Class members' PII.

86. Equifax owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

87. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

88. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class members' PII.

89. Equifax also had independent duties under Plaintiff's and Class members' state laws that required Equifax to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the Data Breach.

90. Equifax had a special relationship with Plaintiff and Class members from being entrusted with their PII, which provided an independent duty of care. Plaintiff and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

91. Equifax's role to utilize and purportedly safeguard consumers' PII presents

unique circumstances requiring a reallocation of risk.

92. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that its data security practices were inadequate to safeguard Class members' PII; and (d) failing to provided adequate and timely notice of the Data Breach.

93. But for Equifax's breach of its duties, Class members' PII would not have been accessed by unauthorized individuals.

94. Plaintiff and Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

95. As a result of Equifax's willful and/or negligent failure to prevent the Data Breach, Plaintiff and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII.

96. The damages to Plaintiff and Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

97. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT IV

NEGLIGENCE PER SE

(on behalf of the Nationwide Class)

98. Plaintiff incorporates by reference all paragraphs above.

99. Under the FCRA, 15 U.S.C. § 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

100. Defendant failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA.

101. Plaintiff and Class members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

102. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> **(1)** to ***insure the security and confidentiality of customer records and information***;
>
> **(2)** to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and
>
> **(3)** to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b) (emphasis added).

103. In order to satisfy their obligations under the GLBA, Equifax also was required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

104. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of

unauthorized access to customer information in customer information systems." *See id.*

105. Further, when Equifax became aware of " unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

106. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to: Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class members' PII.

107. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

108. Equifax also violated the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

109. Plaintiff and Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class members themselves would cause damages to Class members.

110. Defendant's failure to comply with the applicable laws and regulations, including the FCRA and the GLBA, constitutes negligence *per se*.

111. But for Equifax's violation of the applicable laws and regulations, Class members' PII would not have been accessed by unauthorized individuals.

112. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII.

113. The damages to Plaintiff and to Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties under applicable laws and regulations.

114. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT V

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq*.

(on behalf of the California Subclass)

115. Plaintiff incorporates by reference all paragraphs above.

116. California's Unfair Competition Law, California Business & Professions Code § 17200 *et seq.*, prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." For the reasons discussed above, Equifax violated (and continues to violate) this law by engaging in the above-described unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

117. Equifax's unfair and fraudulent acts and practices include but are not

limited to the following:

a. Equifax failed to enact adequate privacy and security measures to protect California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, in violation of industry standards and best practices, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action, following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard Class members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Equifax knowingly and fraudulently misrepresented that it would and did comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' PII;

e. Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for Class members' PII;

f. Equifax failed to maintain reasonable security, in violation of Cal. Civ. Code § 1798.81.5; and

g. Equifax failed to disclose the Data Breach to Class members in a timely and accurate manner, in violation of the duties imposed by Cal. Civ. Code § 1798.82 *et seq*.

118. Equifax's acts and practices also constitute "unfair" business acts and practices, in that the harm caused by Equifax's wrongful conduct outweighs any utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral, unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused and will continue to cause substantial injury to consumers such as Plaintiff and Class members.

119. Equifax's acts and practices also constitute "unlawful" business acts and

practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as described fully above), the GLBA, 15 U.S.C. § 6801 *et seq.* (as described fully above), California's fraud and deceit statutes, Cal. Civ. Code §§ 1572, 1573, 1709, 1711; Cal. Bus. & Prof. Code §§ 17200, *et seq.*, 17500, *et seq.*, the California Customer Records' Act, Cal. Civ. Code §§ 1798.80, *et seq*. (further described below), and California common law.

120. There were reasonably available alternatives to further Equifax's legitimate business interests, including using best practices to protect Class members' PII, other than Equifax's wrongful conduct described herein.

121. As a direct and/or proximate result of Equifax's unfair practices, Plaintiff, the Nationwide Class, and the California Subclass have suffered injury in fact in connection with the Data Breach, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII. As a result, Plaintiff and other Class members are entitled to compensation, restitution, disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code § 17203.

122. Equifax knew or should have known that its data security practices and infrastructure were inadequate to safeguard Class members' PII, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to Class members' rights.

123. On information and belief, Equifax's unlawful and unfair business practices, except as otherwise indicated herein, continue to this day and are ongoing.

124. Plaintiff and Class members also are entitled to injunctive relief, under California Business and Professions Code §§ 17203, 17204, to stop Equifax's wrongful acts and to require Equifax to maintain adequate security measures to protect the personal and financial information in its possession.

125. Under Business and Professions Code § 17200 *et seq.*, Plaintiff seeks

restitution of money or property that the Defendant may have acquired by means of deceptive, unlawful, and unfair business practices (to be proven at trial), restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices (to be proven at trial), declaratory relief, and attorney's fees and costs (allowed by Cal. Code Civil Pro. §1021.5).

COUNT VI

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code § 1798.80, *et seq.*

(On Behalf of the California Subclass)

126. Plaintiff incorporates by reference all paragraphs above.

127. "[T]o ensure that personal information about California residents is protected," Civil Code § 1798.81.5 requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

128. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, about Plaintiff and the California Subclass.

129. Equifax violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect Class members' PII.

130. As a direct and proximate result of Defendant's violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

131. In addition, California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably

believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ."

132. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

133. Equifax is a business that own or license computerized data that includes personal information as defined by Cal. Civ. Code § 1798.80 *et seq.*

134. In the alternative, Equifax maintains computerized data that includes personal information that Equifax does not own as defined by Cal. Civ. Code § 1798.80 *et seq.*

135. Plaintiff's and the California Subclass members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

136. Because Equifax reasonably believed that Plaintiff and the California Subclass members' personal information was acquired by unauthorized persons during the Data Breach, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

137. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

138. As a direct and proximate result of Defendant's violations of sections 1798.81.5 and 1798.82 of the California Civil Code, Plaintiff and California Subclass Members suffered the damages described above, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

139. Plaintiff the California Subclass seek relief under § 1798.84 of the California Civil Code, including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

COUNT VII

VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT

Ga. Code Ann. § 10-1-912, *et seq.*

(On Behalf of the Nationwide Class)

140. Plaintiff incorporates by reference all paragraphs above.

141. Under Ga. Code Ann. § 10-1-912(a), "[a]ny information broker … that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay . . . ."

142. Under Ga. Code Ann. § 10-1-912(b), "[a]ny person or business that maintains computerized data on behalf of an information broker . . . that includes personal information of individuals that the person or business does not own shall notify the information broker . . . of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

143. Equifax is an information broker that owns or licenses computerized data that includes personal information, as defined by Ga. Code Ann. § 10-1-911.

144. In the alternative, Equifax maintains computerized data on behalf of an information broker that includes personal information that Equifax does not own, as defined by Ga. Code Ann. § 10-1-911.

145. Plaintiff's and Class members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under Ga. Code Ann. § 10-1-911(6).

146. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Class members' PII), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

147. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

148. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiff and Class members suffered the damages alleged herein.

149. Plaintiff seeks relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

RELIEF REQUESTED

Plaintiff, individually and on behalf of all others similarly situated, requests that the Court enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class and Statewide Subclasses as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper Class representative;

B. Injunctive relief requiring Defendant to (1) strengthen its data security systems that maintain PII to comply with the FCRA and GLBA, the applicable state laws alleged herein (including but not limited to the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform

internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendant to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiff and all Class (and Subclass) Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiff and all Class (and Subclass) Members of additional credit monitoring and identity theft protection services beyond the one-year package Equifax currently is offering;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity; and

F. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: September 28, 2017

Respectfully submitted,

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson

Tina Wolfson
Robert Ahdoot
Theodore Maya
Bradley K. King
1016 Palm Avenue
West Hollywood, CA 90069
Tel: 310-474-9111
Fax: 310-474-8585